

**REMARKS**

Claims 1, 3-5, 7-12, 14, 19, 20, 22-24, 28-32, 34, 38-41, 48-50, 72, 73, 75-81, 84 and 85 are pending in the application. Claims 1, 3-5, 7-12, 14, 19, 20, 22-24, 28-32, 34, 38-41, 48-50, 72, 73, 75-81, 84 and 85 stand rejected under 35 U.S.C. 103(a).

***Claim Amendments***

The foregoing amendment clarifies the expression of the invention. Support for the amendment is found throughout the specification and in the original claims as detailed below. Accordingly, no new matter has been added. New claim 93 focuses on features of applicants' invention, such as providing the virtual wallet application with a local aspect residing on the owner's computing device and a remote aspect residing on a trusted third party's server (Spec. p. 6, lines 16-26), assigning a primary aspect of the secret access device to the owner by the virtual wallet application for accessing both aspects of the virtual wallet application by the owner via the computing device coupled to the server over a network (Spec. p. 7, lines 6-17), escrowing a secondary aspect of the secret access device by a virtual executor function of the virtual wallet application preprogrammed to utilize the secondary aspect to allow access to the owner's stored data only to an authorized representative of the owner's estate upon verification of an occurrence of a predefined event that renders the owner incapable of acting on the owner's own behalf (Spec. p. 8, line 1-p. 9, line 8), allowing the owner at the computing device to store data relating to the owner's estate on the local aspect of the virtual wallet application (Spec. p. 9, lines 24-28), periodically updating the remote aspect of the virtual wallet application with the data stored on the local aspect by a virtual archivist function of the virtual wallet application via the network (Spec. p. 6, lines 26-28, and if the occurrence of the predefined event is verified, allowing access for the authorized representative of the owner's estate to the owner's stored data by the virtual executor function utilizing the secondary aspect of the secret access device (Spec. p. 9, lines 17-23).

***Claim Rejections - 35 USC § 103***

Claims 1, 3-5, 7-12, 14, 19, 20, 22-24, 28-32, 34, 38-41, 48-50, 72, 73, 75-81, 84 and 85 stand rejected over Fischer (U.S. 6,141,423) in view of Rosen (U.S. 5,453,601) under 35 U.S.C. 103(a). The rejection is respectfully traversed and reconsideration is requested. Fischer in view of Rosen does not teach or suggest the claimed invention either separately or in combination with one another.

Fischer discloses a method and apparatus for preventing a trustee holding escrowed security information from revealing the information to someone other than a party legitimately entitled to receive such information. According to Fischer, in modern computer systems, especially those using a PC or laptop computer, it is common for the data stored in, for example, disk memory to be encrypted. (Fischer, Col 1, lines 18-20). The user's password is converted via well known cryptographic processing techniques into a cryptographic key, which is used to decrypt (and thereby access) all information stored in the computer. (Fischer, Col 25-28) A problem that Fischer sought to address was that users often forget their passwords. According to Fischer, a previous attempt to solve that problem was to "escrow" the password (or some other key information associated with the encryption) with a trustee, i.e., a trusted entity such as, for example, a computer security software officer in the user's organization. (Fischer, Col 1, line 42-45)

In Fischer's approach to solving the problem of lost passwords, various alternative binary data strings may be escrowed. A password used to derive a symmetric DES key which is used to encrypt the user's secret may be escrowed. Fischer contemplates, for example, escrowing any secret digital information voluntarily placed in the hands of an escrow agent (e.g., a Swiss bank account number, safety deposit identifying indicia, vault combination, the formula for Coca Cola® or the like), and Fischer aims to permit the user to cryptographically secure such data and to securely permit a manufacturer, vendor, or other escrow agents (trustee) to allow the user to access data under circumstances where the password is forgotten or lost. (Fischer, Col 2, lines 19-31)

In a definition phase of Fischer, the true owner/customer defines an escrow record which provides self-identification data together with encrypted password or other secret data. (Fischer, Col 2, lines 45-47) If the user forgets the password, a retrieval phase of Fischer is performed, in which the user contacts the escrow agent, e.g., the vendor or manufacturer. The user (applicant) must provide sufficient credentials to definitively establish his or her identification, such as an affidavit executed before a notary public, a digitally signed message verifiable with a well certified public key (or the public key indicated in the escrowed information itself), production of a driver's license, independent investigation by the trustee; or the physical presence of the applicant to confirm identity. In initially establishing the escrow record, the user is asked to define for the vendor what security measures are to be required if the key (or other secret information) must sometimes be retrieved, such as, by requiring identification performed before a notary, a personal appearance, production of a valid driver's license, etc. This allows the true owner to stipulate recovery procedures. (Fischer, Col 3, lines 1-21)

According to Fischer, where the trustee is a vendor providing the key-recovery service, it may be preferred that the user can only extract the escrowed ciphertext with the help of a utility provided by the vendor (at an applicant's request). (Fischer, Col 3, lines 31-34) If the identity is verified, the password is communicated to the requester (who has been appropriately identified) via communication channel 12 in a secure fashion. (Fischer, Col 6, lines 24-27)

Rosen discloses an electronic funds transfer system that utilizes electronic money which is interchangeable with cash and universally accepted. (Rosen, Col. 2, lines 54-54). In the Rosen system, a bank utilizes a computer module to issue electronic money to subscribers that is backed, for example, by demand deposits and accepted by correspondent banks. The subscribers are provided with computer modules for storing the electronic money and performing transactions with the on-line systems of participating banks or exchanging electronic money with one another via their respective computer modules in off-line transactions. Issuing and correspondent banks also use computer modules, for example, for interfacing to subscribers' computer modules and between the issuing and

correspondent banks, and a clearing bank balances the electronic money accounts of the different issuing banks. (Rosen, Col. 3, lines 40-59).

The relevance of the article "Information for Executors and Administrators" is not apparent. According to the article, people rent safe deposit boxes for keeping documents, jewelry, bonds, property deeds, and wills, and then die; banks do not allow third parties access to the dead person's safe deposit box without a death certificate and proof of the third party's authority; and banks are more likely to open safe deposit boxes for family members of the dead person. (P. 9, "Information for Executors and Administrators")

Fischer and/or Rosen are devoid of any teaching or suggestion of features of, and the Information for Executors and Administrators has nothing to do with, applicants' claimed invention, such as a virtual wallet application with local and remote aspects, a primary aspect of a secret access device for accessing both aspects, and a secondary aspect of the secret access device escrowed by a virtual executor function preprogrammed to use the secondary aspect to allow access to the owner's stored data only to an authorized representative of the owner's estate on verification of an occurrence of a predefined event that renders the owner incapable of acting on the owner's own behalf. Nor is there any teaching or suggestion in Fischer and/or Rosen of allowing the owner to store data relating to the owner's estate on the local aspect of the virtual wallet application and periodically updating the remote aspect of the virtual wallet application with data stored on the local aspect by a virtual archivist function of the virtual wallet application. These features are believed to be clearly patentable over the applied prior art. The above-noted aspects are not disclosed or suggested by the references asserted against the claims of record. Specifically, the asserted references fail to provide key features of the invention, and the claimed invention is patentably distinct from the cited references.

The Fischer system is designed and implemented to address a perceived danger that a trustee might be tricked into revealing escrowed information to someone other than the legitimate owner (or another party entitled to receive the escrowed information), such as a thief presenting a stolen computer to the trustee claiming that it is their own, and the Rosen system is designed and implemented as an electronic funds transfer system utilizing electronic money that is interchangeable with cash. The above-noted aspects of applicant's claimed

invention are not disclosed or suggested by Fischer and/or Rosen either separately or in any combination with one another.

**Version With Markings to Show Changes Made**

**Amendments in the Claims:**

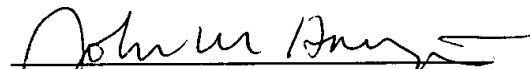
In accordance with 37 CFR 1.121(c)(1)(ii), a marked up version does not have to be supplied for an added or deleted claim.

**Conclusion**

In view of the foregoing amendment and these remarks, each of the claims remaining in the application is in condition for immediate allowance. Accordingly, the examiner is requested to reconsider and withdraw the rejection and to pass the application to issue. The examiner is respectfully invited to telephone the undersigned at (336) 607-7318 to discuss any questions relating to the application.

Respectfully submitted,

Date: 9/18/02

  
John M. Harrington (Reg. No. 25,592)  
for George T. Marcou (Reg. No. 33,014)

Kilpatrick Stockton LLP  
607 14<sup>th</sup> Street, NW, Suite 900  
Washington, DC 20005  
(202) 508-5800

T0091-178714  
WINLIB01:968945.1